SIMPT
Svenska institutet mot penningtvätt
Swedish Anti-Money Laundering Institute

Grundläggande vägledning om allmän riskbedömning

Femte upplagan

Det har gjorts en översyn av denna vägledning. Vägledningen har omarbetats, utvecklats och uppdaterats. En del text har flyttats från processbeskrivningen (del II) till metodbeskrivningen (del I).

Nuvarande vägledning finns här:
https://www.simpt.se/media/1326/grundlaeggande-vaegledning-allmaen-riskbedoemning-4-uppl.pdf

Öppen konsultation juni 2023

Innehållsförteckning

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 femte upplaga har vägledningen omarbetats, uppdaterats och utvecklats i flera delar.

Inledning

Syftet med denna vägledning är att beskriva vad som krävs enligt penningtvättsregelverket i fråga om att göra en allmän riskbedömning. I vägledningen beskrivs också – på ett grundläggande sätt – dels en metod som kan användas för att göra den allmänna riskbedömningen i praktiken (del I), dels några särskilda processfrågor som kan uppstå i arbetet (del II).

Vägledningen är inte avsedd att användas som en mall, utan som ett stöd för verksamhetsutövaren i det egna arbetet med att göra en allmän riskbedömning. Den allmänna riskbedömningen och metoden för att göra denna måste alltid anpassas efter den egna verksamheten.

Allmän riskbedömning handlar om att bedöma risken för att verksamheten utnyttjas för penningtvätt och finansiering av terrorism. Den allmänna riskbedömningen ska utgöra grunden för verksamhetsutövarens riskbaserade förhållningssätt, som ska genomsyra tillämpningen av penningtvättsregelverket. Verksamhetsutövaren har stor valfrihet i hur arbetet med den allmänna riskbedömningen genomförs.

Riskbedömningen är viktig för flera 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, som 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).

Det riskbaserade förhållningssättet

Den allmänna riskbedömningen ska utgöra grunden för verksamhetsutövarens riskbaserade förhållningssätt, som ska genomsyra tillämpningen av penningtvättsregelverket.

Det svenska penningtvättsregelverket utgår från internationella åtaganden och bygger på EU-direktiv, 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. I rekommendationerna lyfts det riskbaserade förhållningssättet fram som en viktig grund för en effektiv fördelning av resurser (rekommendation 1). Det fjärde penningtvättsdirektivet (2015/849) genomsyras i högre grad än tidigare direktiv av principen om ett riskbaserat förhållningssätt.

Utmärkande för Fatf:s 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). Syftet med penningtvättsregelverket innebär ytterst att verksamhetsutövarna bidrar till arbetet med att förebygga och upptäcka brottslig verksamhet. I linje med vad som följer av de internationella regelverken, ska verksamhetsutövarnas åtgärder för att uppnå detta syfte utgå från ett riskbaserat förhållningssätt.

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.

Omfattningen av åtgärder, förfaranden och kontroller för att förhindra att verksamheten utnyttjas för penningtvätt och finansiering av terrorism ska utformas och löpande 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. 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).

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 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 verksamhetsutövaren kan och faktiskt vidtar åtgärder för att hantera riskerna.

I Eba:s riktlinjer för riskfaktorer, riktlinjerna 4.9-4.11, tas frågan om tillgång till finansiella tjänster upp. Där framgår bl.a. att eftersom riskerna med enskilda affärsförbindelser varierar, även inom en kategori, kräver en riskbaserad metod inte att företaget ska vägra eller avsluta affärsförbindelser med hela kundkategorier som förknippas med förhöjd risk för penningtvätt och finansiering av terrorism. Företaget bör noggrant balansera behovet av tillgång till finansiella tjänster och behovet av att minska risken för penningtvätt och finansiering av terrorism. Detta inbegriper att ett företag bör införa lämpliga och riskbaserade riktlinjer och åtgärder för att säkerställa att dess metod för att vidta åtgärder för kundkännedom inte medför att legitima kunder otillbörligt vägras tillgång till finansiella tjänster, Guidelines ML TF Risk Factors_SV.pdf (europa.eu).

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, se Fatf Guidance for a Risk-Based Approach the Banking Sector s. 6 RISK-BASED APPROACH GUIDANCE FOR THE BANKING SECTOR (fatf-gafi.org)

Regelverket

Penningtvättslagen

Enligt 2 kap. 1 § penningtvättslagen ska en verksamhetsutövare göra en allmän riskbedömning. Det innebär att det ska göras 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 misstänkta aktiviteter och transaktioner samt till information om tillvägagångssätt för penningtvätt och finansiering av terrorism och andra relevanta uppgifter som myndigheter lämnar. Detta innebär att verksamhetsutövare är skyldiga att beakta information som tillhandahålls av tillsynsmyndigheter, brottsbekämpande myndigheter och andra myndigheter (prop. 2016/17:173 s. 510).

Enligt 2 kap. 2 § penningtvättslagen ska omfattningen av den allmänna riskbedömningen bestämmas med hänsyn till verksamhetsutövarens storlek och art och de risker för penningtvätt eller finansiering

av terrorism som kan antas föreligga. Riskbedömningen ska utformas så att den kan ligga till grund för verksamhetsutövarens rutiner, riktlinjer och övriga åtgärder mot penningtvätt och finansiering av terrorism. Den allmänna riskbedömningen ska dokumenteras och hållas uppdaterad.

Den allmänna riskbedömningen ligger till grund för flera åtgärder som ska vidtas enligt penningtvättslagen:

- **Kundens riskprofil:** Verksamhetsutövaren ska bedöma den risk för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen (kundens riskprofil). Kundens riskprofil ska bestämmas med utgångspunkt i den allmänna riskbedömningen och verksamhetsutövarens kännedom om kunden (2 kap. 3 § penningtvättslagen).
- **Kundkännedom:** Verksamhetsutövarens åtgärder för kontroll, bedömning och utredning enligt 3 kap. 7, 8 och 10-13 §§ penningtvättslagen, dvs. åtgärder för kundkännedom, ska utföras i den omfattning det behövs med hänsyn till kundens riskprofil och övriga omständigheter (3 kap. 14 § penningtvättslagen). Kundens riskprofil ska, som framgår ovan, bestämmas bl.a. med utgångspunkt i den allmänna riskbedömningen.
- **Övervakning:** Verksamhetsutövaren ska övervaka pågående affärsförbindelser i syfte att upptäcka avvikande aktiviteter och transaktioner. Inriktningen och omfattningen av övervakningen ska bestämmas med beaktande av de risker som identifierats i den allmänna riskbedömningen, den risk för penningtvätt och finansiering av terrorism som kan förknippas med kundrelationen och annan information om tillvägagångssätt för penningtvätt eller finansiering av terrorism (4 kap. 1 § penningtvättslagen).
- **Intern kontroll och modellriskhantering:** Verksamhetsutövaren ska ha rutiner och riktlinjer för intern kontroll. Om en verksamhetsutövare använder modeller för bl.a. riskbedömning, ska verksamhetsutövaren ha rutiner för modellriskhantering. Rutinerna för modellriskhantering ska syfta till att utvärdera och kvalitetssäkra de modeller som verksamhetsutövaren använder. Omfattningen av och innehållet i rutinerna och riktlinjerna ska bestämmas med hänsyn till verksamhetsutövarens storlek och art samt den risk för penningtvätt och finansiering av terrorism som identifierats i den allmänna riskbedömningen (6 kap. 1 § penningtvättslagen).
- **Rutiner och riktlinjer:** Verksamhetsutövaren ska ha dokumenterade rutiner och riktlinjer avseende sina åtgärder för kundkännedom, övervakning och rapportering samt för behandling av personuppgifter. Rutinerna och riktlinjerna ska fortlöpande anpassas efter nya och förändrade risker för penningtvätt och finansiering av terrorism. Rutinernas och riktlinjernas omfattning och innehåll ska bestämmas med hänsyn till verksamhetsutövarens storlek, art och riskerna för penningtvätt och finansiering av terrorism som identifierats i den allmänna riskbedömningen (2 kap. 8 § penningtvättslagen).

Penningtvättsföreskrifterna

Enligt 2 kap. 1 § penningtvättsföreskrifterna ska företaget 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.

Enligt Finansinspektionens beslutspromemoria till penningtvättsföreskrifterna får en riskbedömning för en verksamhet med ett fåtal okomplicerade produkter och tjänster vara mindre omfattande än för

ett företag med komplicerade eller med ett större utbud av produkter och tjänster (FI Dnr 16–2467 s. 10).

Eba:s riktlinjer för riskfaktorer

Verksamhetsutövare ska beakta Eba:s riktlinjer för riskfaktorer, som gäller som allmänna råd. Innehållet i riktlinjerna återges här i vissa delar. I övrigt hänvisas till riktlinjerna, Guidelines ML TF Risk Factors_SV.pdf (europa.eu)

Enligt Eba:s riktlinjer för riskfaktorer bör företaget säkerställa att det har en grundlig insikt i de risker för penningtvätt och finansiering av terrorism som det exponeras för (riktlinje 1.1).

Den allmänna riskbedömningen bör hjälpa företaget att förstå sin exponering för riskerna för penningtvätt och finansiering av terrorism och vilka delar av dess verksamhet det bör prioritera för att bekämpa penningtvätt och finansiering av terrorism. Företaget bör därför ha en helhetssyn på riskerna genom att identifiera och bedöma de risker som förknippas med de produkter och tjänster som det erbjuder, de länder och geografiska områden som det verkar inom, de kunder som söker sig till det och de distributionskanaler som det använder för att betjäna sina kunder (riktlinjerna 1.11 och 1.12).

Den allmänna riskbedömningen omfattar en bedömning av den risk för penningtvätt och finansiering av terrorism som företaget exponeras för på grund av verksamhetens art och komplexitet (riktlinje 1.2). Metoden för att göra den allmänna riskbedömningen behöver anpassas efter den verksamhet som bedrivs och göras i proportion till företagets storlek och art (se riktlinje 1.16).

I riktlinje 1.16 framhålls små företag som inte erbjuder några komplicerade produkter eller tjänster eller vars exponering är begränsad eller endast inhemsk som verksamhetsutövare som möjligen inte behöver göra någon överdrivet komplicerad eller avancerad riskbedömning.

Verksamhetsutövaren bör alltid dokumentera sin allmänna riskbedömning och alla förändringar som görs på ett sätt som möjliggör för både verksamhetsutövaren och myndigheter att förstå hur den genomfördes och varför den genomfördes på ett visst sätt (riktlinje 1.4).

Det bör framhållas att enligt riktlinje 1.5 bör ett företag som är kreditinstitut eller värdepappersföretag i detta sammanhang även beakta Eba:s riktlinjer för intern styrning (EBA/GL/2017/11).

Se mer om Eba:s riktlinjer för riskfaktorer i avsnittet nedan, Del I - En metodbeskrivning.

Förarbetena till penningtvättslagen (prop. 2016/17:173)

I förarbetena till penningtvättslagen (prop. 2016/17:173) framgår bl.a. följande.

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).

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 §§ penningtvättslagen (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).

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, och prop. 2016/17:173 s. 209).

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).

Vid riskklassificeringen av enskilda kundrelationer har verksamhetsutövaren 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 (prop. 2016/17:173 s. 260).

Den allmänna riskbedömningen ska omfatta både risken för penningtvätt och finansiering av terrorism

Penningtvätt

Penningtvätt definieras i 1 kap. 6 § penningtvättslagen.

Penningtvätt definieras som 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

Finansiering av terrorism definieras i 1 kap. 7 § penningtvättslagen.

Finansiering av terrorism definieras som sådan insamling eller sådant mottagande eller tillhandahållande av pengar eller annan egendom som avses i 6 § terroristbrottslagen (2022:666).

Definitionen träffar därmed, enligt 6 § terroristbrottslagen, 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 prop. 2021/22:133 s. 232.

Skillnader mellan penningtvätt och finansiering av terrorism

Den allmänna riskbedömningen ska fokusera både på riskerna för penningtvätt och för finansiering av terrorism. Den gemensamma nämnaren är utnyttjandet av det finansiella systemet för illegala ändamål. Detta är också anledningen till att åtgärder mot penningtvätt och finansiering av terrorism ofta behandlas i samma kontext. 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).

Penningtvätt syftar alltså till att dölja medels ursprung, medan det vid finansiering av terrorism i huvudsak handlar om att dölja vad pengarna ska användas till. Denna grundläggande skillnad gör att det finns anledning 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. 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 (se den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 23).

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 kan kräva 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 bl.a. 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.

Del I – En metodbeskrivning

Begreppskatalog

Här beskrivs begrepp – i bokstavsordning – såsom de används i vägledningen.

BEGREPP	BESKRIVNING
Hot	En person, grupp eller aktivitet/handling som kan innebära en risk för att verksamheten utnyttjas för penningtvätt och finansiering av terrorism (jfr den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021). Aktiviteter eller handlingar som kan främja eller leda till penningtvätt eller finansiering av terrorism, kan betecknas som hotaktiviteter. Individer eller organisationer som utför hotaktiviteter kan betecknas som hotaktörer.

	Bedömningen av hot kan göras utifrån olika aktiviteter som kan vara del av penningtvätts- och terrorismfinansieringsupplägg. Det handlar om värdeomvandlande aktiviteter, värdeöverförande och värdeförflyttande aktiviteter, värdebevarande aktiviteter samt värdegenererande aktiviteter. I bedömningen av hot görs en bedömning av hur, dvs. på vilket sätt, en riskfaktor innebär en risk för att verksamheten kan utnyttjas för penningtvätt eller finansiering av terrorism.
Inneboende risk	Risknivån före riskreducering, dvs. risken för att 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, innan mitigerande åtgärder har vidtagits. Se också Eba:s riktlinjer för riskfaktorer, avsnitt 2.12 c.
Konsekvens	En bedömning av den påverkan som ett utnyttjande av verksamheten kan få.
Mitigerande åtgärd	Åtgärd för att minska risken till en nivå där risken för att verksamheten ska utnyttjas för penningtvätt och finansiering av terrorism kan hanteras eller kontrolleras. Även kallat kontrollåtgärd.
Residualrisk	Den risknivå som kvarstår efter att mitigerande åtgärder har vidtagits. Även kallat kvarstående risk. Se också Eba:s riktlinjer för riskfaktorer, avsnitt 2.12 h.
Riskexponering	Den samlade riskbilden, grundad på en bedömning av sannolikhet och konsekvens, innan mitigerande åtgärder har vidtagits.
Riskfaktor	Variabler som antingen enskilt eller i kombination kan öka eller minska den risk för penningtvätt och finansiering av terrorism som är förknippad med en enskild affärsförbindelse eller en enstaka transaktion (Eba:s riktlinjer för riskfaktorer, avsnitt 2.12 k).
Riskkategori/ risksegment	Begrepp som används för övergripande riskområden, såsom produkt och tjänst, kunder, distributionskanaler och geografi.
Sannolikhet	En bedömning av hur stor sannolikheten är för att penningtvätt eller finansiering av terrorism sker genom ett utnyttjande av verksamheten. Bedömningen bör göras utifrån verksamhetens omfattning i relation till en riskfaktor.
Sårbarhet	Förhållanden som utgör svaga punkter i verksamheten och som därmed innebär att hot kan realiseras (jfr den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021). En sårbarhet kan vara en systemdel som saknas eller vars funktion bedöms utgöra ett problem för möjligheten att förhindra penningtvätt eller finansiering av terrorism. I bedömningen av sårbarhet görs en bedömning av varför det finns en risk för att verksamheten utnyttjas för penningtvätt eller finansiering av terrorism, dvs. varför det finns en risk för att hoten realiseras.

Begreppet risk

Begreppet risk kan bygga på olika parametrar, beroende på sammanhang.

I förarbetena till penningtvättslagen anges att riskbegreppet i första hand innebär 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).

I Eba:s riktlinjer för riskfaktorer, avsnitt 2.12 i, definieras risk som sannolikheten för att penningtvätt och finansiering av terrorism ska äga rum samt dess påverkan om så sker.

I den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021 s. 122 anges att enligt Financial Action Task Force, Fatf, är risk en funktion av tre faktorer: hot, sårbarhet och konsekvens. Enligt Fatf är det upp till landet själv att författa en produkt eller process baserad på en metod som beslutas av landets berörda parter. Definitionerna för hot, sårbarhet och konsekvens är lämpliga att utgå ifrån.

Metoden som beskrivs i denna vägledning för att göra den allmänna riskbedömningen utgår också från att en bedömning görs av hot, sårbarhet, sannolikhet och konsekvens. Som framgår i det följande förekommer i praktiken också andra begrepp än hot och sårbarhet, t.ex. riskhöjande och risksänkande faktorer.

Generellt sett används tre risknivåer vid riskbedömningen, både vad avser den inneboende risken och residualrisken. Risknivåerna är låg, medel (normal) och hög risk. Det är inget som hindrar ytterligare nivåer, t.ex. olika nivåer inom medelrisk eller ytterligare nivåer av hög risk. En sådan indelning kan ytterligare underlätta för företaget att bestämma åtgärder för att hantera riskerna.

Inledning till metodbeskrivningen

Det finns en stor valfrihet i hur verksamhetsutövaren gör sin allmänna riskbedömning.

Vissa företag kan göra en allmän riskbedömning som inte är överdrivet komplicerad eller avancerad (Eba:s riktlinjer för riskfaktorer, riktlinje 1.16). 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).

Ett företag som däremot har t.ex. ett stort produkt- och tjänsteutbud eller mer komplicerade produkter och tjänster kan behöva göra en mer avancerad riskbedömning. I dessa fall kan det underlätta arbetet om riskbedömningen görs i olika underprocesser innan allt läggs samman i det som blir den allmänna riskbedömningen. Detta är inte något krav, utan endast ett sätt att underlätta det praktiska arbetet med att göra den allmänna riskbedömningen i en större eller mer komplex verksamhet, inte minst om olika kompetenser behövs för de olika delarna av riskbedömningen.

Den allmänna riskbedömningen ska beskriva de inneboende riskerna, dvs. risken för att 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. Det riskbaserade förhållningssättet utgår dock inte bara från att riskerna identifieras och bedöms utan bygger i praktiken också på att åtgärder vidtas och

löpande anpassas för att mitigera riskerna, vilket ger en residualrisk. Residualrisken beskriver den kvarstående, faktiska risk som finns i verksamheten, efter att mitigerande åtgärder har vidtagits. Den allmänna riskbedömningen ska kunna ligga till grund för en effektiv allokering av resurserna, flest och mest omfattande åtgärder ska sättas in där riskerna är som störst. Detta innebär att även åtgärderna och de risker som kvarstår och som verksamheten faktiskt är exponerad för, dvs. residualrisken, behöver kartläggas och synliggöras.

Den metod som beskrivs i denna vägledning är på en grundläggande nivå och indelad i tre faser. Metodbeskrivningen är inte avsedd att användas som en mall, utan som ett stöd för verksamhetsutövaren i det egna arbetet med att göra en allmän riskbedömning. Varje verksamhetsutövare behöver ha en metod som är anpassad efter den egna verksamheten och ett riskbaserat förhållningssätt (jfr Eba:s riktlinjer för riskfaktorer, riktlinje 1.16).

Metodens tre faser:

- **I fas 1** bedöms den inneboende risken. Bedömningen kan göras i tre steg. Först identifieras riskfaktorer via externa och interna källor. Sedan görs en bedömning av hur, varför och i vilken omfattning som riskfaktorerna påverkar den inneboende risken, dvs. risken för att verksamheten utnyttjas för penningtvätt och finansiering av terrorism innan mitigerande åtgärder har vidtagits. Därefter görs en bedömning av sannolikhet och konsekvens samt en sammantagen bedömning av verksamhetens riskexponering. Riskexponeringen visar de risker som verksamheten faktiskt är exponerad för och hur stor risken i realiteten är innan mitigerande åtgärder har vidtagits.
- **I fas 2** bedöms effektiviteten i de mitigerande åtgärder som har vidtagits för att hantera den inneboende risken. Det kan göras i två steg. Först identifieras åtgärder sedan görs en bedömning av hur effektivt åtgärderna har hanterat den inneboende risken.
- **I fas 3** bedöms residualrisken. Residualrisken beskriver den risknivå som kvarstår efter riskreducering, dvs. efter att mitigerande åtgärder har vidtagits, även kallat kvarstående risk.

Sammanfattning av metodens tre faser

TRE FASER I ARBETET MED ALLMÄN RISKBEDÖMNING
1. Bedöma den inneboende risken Kan göras i tre steg: 1) Identifiera riskfaktorer via externa och interna källor 2) Bedöma hur, varför och i vilken omfattning som respektive riskfaktor påverkar eller driver risken för att verksamheten ska utnyttjas för penningtvätt och finansiering av terrorism. 3) Bedöma sannolikhet, konsekvens och riskexponering
2. Bedöma effektiviteten i de mitigerande åtgärder som har vidtagits för att hantera den inneboende risken Kan göras i två steg: 1) Identifiera åtgärder 2) Bedöma hur effektivt åtgärderna har hanterat den inneboende risken
3. Bedöma residualrisken

Fas 1: Bedöma den inneboende risken

Inledning

Inneboende risk är risken för att verksamheten utnyttjas för penningtvätt och finansiering av terrorism, såsom den bedöms innan mitigerande åtgärder har vidtagits.

För att kunna bedöma den inneboende risken bör verksamhetsutövaren ställa sig frågan hur ett utnyttjande skulle kunna gå till och vad som faktiskt kan inträffa i verksamheten. Med utgångspunkt i den inneboende risken ska åtgärder vidtas för att mitigera den inneboende risken. Den risk som sedan återstår är residualrisken.

Den inneboende risken kan bedömas i tre steg.

- **I steg 1** identifieras och sammanställs de riskfaktorer som kan påverka den inneboende risken.
- **I steg 2** görs en bedömning av hur, varför och i vilken omfattning som respektive riskfaktor påverkar eller driver risken för att verksamheten ska utnyttjas för penningtvätt och finansiering av terrorism.
- **I steg 3** görs en bedömning av hur stor sannolikheten är för att penningtvätt eller finansiering av terrorism ska äga rum genom ett utnyttjade av verksamheten och en bedömning görs av konsekvenserna. Det görs också en sammantagen bedömning av verksamhetens riskexponering, dvs. vilka risker som verksamheten faktiskt är exponerad för och hur stor risken i praktiken är före riskmitigering.

Steg 1: Identifiera riskfaktorer

Riskfaktorer

Riskfaktorer är variabler som kan öka eller minska den risk för penningtvätt och finansiering av terrorism som är förknippad med en enskild affärsförbindelse eller en enstaka transaktion. Riskfaktorer kan vara sådant som att kunden är en privatkund eller företagskund, att kundens ägarstruktur är komplex och framstår som ovanlig eller alltför komplicerad för dess verksamhet, att företaget har säte i Sverige, utanför EES eller i ett högrisktredjeland eller att affärsförbindelsen ingås på distans (jfr prop. 2016/17:173 s. 207 och 247). I Eba:s riktlinjer för riskfaktorer ges också exempel på riskfaktorer, se nedan.

Interna och externa källor

För att identifiera de riskfaktorer som påverkar den inneboende risken används både interna och externa källor.

Med *interna källor* avses informationskällor i den egna verksamheten. Det är sådant som har identifierats och analyserats i transaktionsövervakningen, vid rapporteringen till Finanspolisen, vid analysen av kundbeteenden av kundansvariga eller av personer med olika specialistkunskaper. Det kan också vara information från bedömningar som har gjorts i andra sammanhang i fråga om riskfaktorer som också kan vara relevanta för den allmänna riskbedömningen.

Det är inte bara den kunskap som har erhållits vid rapportering utan även den som fås 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.

Med *externa källor* avses informationskällor som finns utanför verksamheten och som framför allt identifieras via omvärldsbevakning.

Som exempel kan utlandsbetalningar och kontanter ha identifierats i externa källor som något som förekommer i olika upplägg för penningtvätt och finansiering av terrorism. Utlandsbetalningar och kontanter kan dock också ha identifierats internt som något som förekommer i samband med avvikande transaktionsmönster. Om det inte är samma personer som gör omvärldsanalysen som hämtar in information från interna källor, bör omvärldsanalysen förmedlas till dem som hämtar in information från interna källor.

Verksamhetsutövaren bör dokumentera de källor som har bedömts vara relevanta.

Externa källor – ej uttömmande (se också Eba:s riktlinjer för riskfaktorer, riktlinjerna 1.29-1.32)

- 2 kap. 4 och 5 §§ penningtvättslagen.
- Bilaga II och III till det fjärde penningtvättsdirektivet, (EU) 2015/849.
- Eba:s riktlinjer för riskfaktorer Guidelines ML TF Risk Factors_SV.pdf (europa.eu)
- Information från Samordningsfunktionen för åtgärder mot penningtvätt och finansiering av terrorism Samordning mot penningtvätt och finansiering av terrorism | Polismyndigheten (polisen.se), bl.a. den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige Rapporter | Polismyndigheten (polisen.se)
- Information från Brottsförebyggande rådet (BRÅ), bl.a. Brå rapport 2021:6 Finansiering av terrorism, En studie av motåtgärder Finansiering av terrorism. En studie av motåtgärder (bra.se)
- De helårsbedömningar som görs av Nationellt centrum för terrorhotbedömning (NTC) Nationellt centrum för terrorhotbedömning - Säkerhetspolisen (sakerhetspolisen.se)
- Annan myndighetsinformation, bl.a. från Finansinspektionen www.fi.se/penningtvatt, Polismyndigheten Finanspolisen | Polismyndigheten och Säkerhetspolisen Publikationer - Säkerhetspolisen (sakerhetspolisen.se)
- 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) https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:52022DC0554&from=EN
- Europeiska bankmyndighetens (Eba) yttrande om de risker för penningtvätt och finansiering av terrorism som påverkar unionens finansiella sektor (EBA/Op/2021/04) Opinion on MLTF risks.pdf (europa.eu)
- Information från andra källor, bl.a. Fatf, www.fatf-gafi.org, Wolfsberg, www.wolfsberg-principles.com, och den amerikanska hemsidan www.fincen.gov, för att få information om bl.a globala, regionala och lokala risker, men även andra risker, se t.ex. Fatfs rapport Professional Money Laundering PROFESSIONAL MONEY LAUNDERING (fatf-gafi.org)
- Övriga källor, t.ex. den vägledning som finns i Storbritannien, www.jmlsg.org.uk

Riskfaktorerna sammanställs och kategoriseras

Enligt 2 kap. 1 § andra stycket penningtvättslagen ska det i den allmänna riskbedömningen särskilt beaktas vilka slags produkter och tjänster som tillhandahålls, vilka kunder och distributionskanaler som finns och vilka geografiska riskfaktorer som föreligger. I vägledningen används begreppet riskkategorier för dessa mer övergripande riskområden. Risksegment är ett annat begrepp som förekommer i praktiken. Enligt penningtvättslagen ska nämnda riskområden/riskkategorier särskilt beaktas. Det finns alltså inget som hindrar att en bedömning görs utifrån ytterligare riskkategorier än de som framgår av penningtvättslagen. De riskfaktorer som har identifierats i interna och externa källor kan sammanställas utifrån riskkategorierna.

Vissa riskfaktorer kan ha betydelse inom flera riskkategorier. Exempelvis kan kontanter vara en riskfaktor i riskkategorin produkt och tjänst. Riskfaktorn kan även vara relevant i riskkategorin kunder, t.ex. om kunderna är verksamma inom en kontantintensiv bransch.

I Eba:s riktlinjer för riskfaktorer anges olika riskfaktorer per riskkategori, se riktlinjerna 2.1-2.21. Här ges några exempel som framgår av riktlinjerna.

Exempel på riskfaktorer per riskkategori

RISKKATEGORI	RISKFAKTORER
Produkt och tjänst Eba:s riktlinjer för riskfaktorer, riktlinjerna 2.16-2.19	Den nivå av insyn eller avsaknad av insyn som produkten eller tjänsten medger (tillåter). Produktens eller tjänstens komplexitetsgrad. I vilken utsträckning som produkten eller tjänsten medger (tillåter) anonymitet. I vilken utsträckning som det är möjligt för tredje part att ge anvisningar. I vilken utsträckning som produkterna eller tjänsterna är kontantintensiva. I vilket utsträckning som produkterna eller tjänsterna medger utlandsbetalningar/gränsöverskridande transaktioner.
Kunder Eba:s riktlinjer för riskfaktorer, riktlinjerna 2.1-2.8	Kundens och den verkliga huvudmannens kopplingar till olika sektorer/branscher, t.ex. kontantintensiva sektorer. Kundens och den verkliga huvudmannens geografiska kopplingar. Kunden eller kundens verkliga huvudman är person i politiskt utsatt ställning.
Geografi	Var verksamhetsutövaren bedriver sin verksamhet.

Eba:s riktlinjer för riskfaktorer, riktlinjerna 2.9-2.15	Var kunderna och deras verkliga huvudmän är baserade eller bosatta och var de har sina huvudsakliga verksamhetsställen; t.ex. inom EES, i högrisländer eller i högrisktredjeländer.
Distributionskanaler Eba:s riktlinjer för riskfaktorer, riktlinjerna 2.20 och 2.21.	Hur affärsförbindelsen inleds och hur kunden identifieras, t.ex. i vilken utsträckning affärsförbindelsen hanteras på distans. Eventuella mellanhänder eller samarbetspartners som företagen använder. Hur produkterna och tjänsterna tillgängliggörs samt transaktioner möjliggörs, t.ex. om kunden kan genomföra transaktioner på egen hand eller om kunden måste kontakta verksamhetsutövaren inför en transaktion.

Steg 2: Bedöma hur, varför och i vilken omfattning riskfaktorerna påverkar risken

Inledning

Bedömningen av hur och varför riskfaktorerna påverkar risken kan göras genom en bedömning av ”hot” och ”sårbarheter”. Dessa begrepp används dock inte alltid. Andra begrepp som kan användas är t.ex. risksänkande och riskhöjande faktorer. Även när dessa begrepp används görs normalt sett en bedömning av hur och varför en riskfaktor medför en risk för att verksamheten utnyttjas. Det innebär att även om begreppen skiljer sig åt kan metoden i grunden vara densamma.

Riskfaktorerna kan åsättas ett värde, som indikerar i vilken omfattning faktorn innebär en risk för penningtvätt eller finansiering av terrorism. En riskfaktor kan innebära en viss risknivå sedd för sig själv, men i kombination med andra faktorer en annan nivå.

Hur utgör riskfaktorn en risk för att verksamheten utnyttjas – hotet?

När en riskfaktor analyseras identifieras hur den medför en risk för att verksamheten utnyttjas för penningtvätt och finansiering av terrorism. Detta kan göras genom en analys och bedömning av hur riskfaktorn utgör ett ”hot” mot verksamheten eller hur den ökar eller minskar risken.

I den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021, s. 122, anges att ett hot är en person, grupp eller verksamhet som kan skada till exempel staten, samhället eller ekonomin. Hotet kan avse kriminella aktörer och deras medhjälpare samt tillgångar och verksamheter. Hot fungerar ofta som en viktig utgångspunkt för att utveckla en förståelse för risken för penningtvätt och finansiering av terrorism. För att kunna göra riskbedömningen är det därför viktigt att ha kännedom om hela kedjan. För penningtvätt är det nödvändigt att förstå både förbrotten och brottsvinsterna samt sedan själva processen med att tvätta brottsvinsterna. För terrorismfinansiering behövs en förståelse både för medlens ursprung och hur de används för att finansiera terrorism.

Analysen av hoten för en verksamhet kan, men behöver inte, göras utifrån olika tillvägagångssätt för att utnyttja verksamheten (hotaktiviteter) eller utifrån vilka typer av aktörer (hotaktörer) som kan utnyttja verksamheten. Att utgå från olika aktiviteter är ett sätt att kategorisera hoten. Ett penningtvätts- eller terrorismfinansieringsupplägg kan bestå av en sekvens av hotaktiviteter.

Exempel på aktiviteter per kategori (se vidare penningtvätt, en nationell riskbedömning, 2013):

- Värdeomvandlande aktiviteter; exempelvis köp av tillgångar av olika slag eller växling.
- Värdeöverförande och värdeförflyttande aktiviteter; exempelvis banköverföring eller kontantsmuggling Värdebevarande aktiviteter; exempelvis lagring av brottsvinster eller registrering av innehav av olika slag.
- För terrorismfinansiering tillkommer värdegenererande aktiviteter; exempelvis insamling av pengar på olika sätt, såsom upptagande av lån eller olika former av brott.

När det gäller skillnaden mellan värdeöverförande och värdeförflyttande aktiviteter bedöms det – mot bakgrund av de exempel som ges i den nationella riskbedömningen från 2013 – handla om å ena sidan överföringar som sker digitalt, dvs. i det finansiella systemet, och å andra sidan ”fysiska” förflyttningar av värden.

Varje riskfaktor måste inledningsvis analyseras var 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 alltså 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 produkten utgör en risk för att utnyttjas för penningtvätt eller finansiering av terrorism. Den individuella bedömningen ska därmed utmynna i en bedömning av vilka brottsliga tillvägagångssätt som är tänkbara.

I förarbetena till penningtvättslagen anges att för att den allmänna riskbedömningen ska vara relevant och tillförlitlig ska den 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).

Fokus för analysen bör vara på verkliga hot. Det är inte effektivt att försöka bedöma allt som kan tänkas hända. Hotanalysen bör därmed utgå från en rimlighetsbedömning av vad som kan inträffa och inte rent hypotetiska eller alltför teoretiska risker för att utnyttjas. Den allmänna riskbedömningen ska utgöra grunden för de åtgärder som vidtas, det är därför viktigt att utgå från de produkter och tjänster som erbjuds i verksamheten och de kunder som verksamheten vänder sig till. Det är 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 och realistisk möjlighet att exempelvis en viss produkt skulle kunna utnyttjas för penningtvätt eller finansiering av terrorism, kan vara grund för att vidta åtgärder.

Varför utgör riskfaktorn en risk för att verksamheten utnyttjas – sårbarheten?

Vid bedömningen av den inneboende risken är det också centralt att bedöma varför det finns en risk för att verksamheten utnyttjas. Det görs en bedömning av om hotet är relevant för verksamheten och vad det i så fall är som gör att verksamheten riskerar att utnyttjas. Detta kan benämnas som verksamhetens ”sårbarhet” inför hotet eller varför en riskfaktor minskar eller ökar risken. Här kan frågan ställas vad som kan göra produkten eller tjänsten mer eller mindre attraktiv ur ett penningtvätts- och terrorismfinansieringsperspektiv och vad som kan påverka verksamhetsutövarens förmåga att upptäcka misstänkt penningtvätt och finansiering av terrorism i förhållande till hotet.

I den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021, s. 122, anges att begreppet sårbarhet syftar på de faktorer som kan utnyttjas av den organisation eller de individer som utgör ett hot eller som kan stödja eller underlätta dess verksamhet. Sårbarhet är i detta sammanhang de förhållanden som utgör svaga punkter i olika system, eller ett visst lands särdrag. Det kan också röra sig om egenskaper hos en viss bransch, finansiell produkt eller typ av tjänst som gör den intressant för personer som vill tvätta pengar eller finansiera terrorism.

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.

En sårbarhet relaterar normalt sett till specifika hot tänkta eller faktiskt föreliggande. Det finns också sådana sårbarheter som är av mer generell karaktär och som är relevanta för en bred uppsättning hot, exempelvis möjligheten att få tillgång till stora mängder kontanter eller en systemdel som saknas eller vars funktion bedöms utgöra ett problem för möjligheten att förhindra penningtvätt eller finansiering av terrorism. Riskfaktorer kan påverka varandra och påverka risken i kombination med varandra

Riskfaktorer kan påverka varandra, dvs. påverka risken med andra riskfaktorer. Som exempel behöver möjligheterna att dölja sambandet mellan egendom och brottet inte ha att göra med en produkts utformning, utan i stället kan sättet för att genomföra en betalning innebära en risk för produkten, genom att överföringen inte är tillräckligt spårbar. Riskfaktorer kan påverka varandra inom alla riskkategorier. Riskfaktorer kan också påverka risken när de förekommer i kombination med varandra.

Exempel – gränsöverskridande transaktion

Gränsöverskridande transaktion kan – enligt information från externa källor – vara en riskfaktor, både vad avser penningtvätt och finansiering av terrorism. Transaktionerna kan bl.a. göra det svårare att spåra medlen och att inhämta information om mottagaren. Medlen kan också skickas till områden förknippade med terrorism eller till områden som är närliggande till sådana områden.

En gränsöverskridande transaktion kan vara en produkt eller tjänst i sig. Riskfaktorn kan också påverka risken med andra riskfaktorer, t.ex. med ett transaktionskonto där gränsöverskridande transaktioner är möjliga att genomföra.

Riskfaktorn kan dessutom påverka risken för att verksamheten utnyttjas för penningtvätt och finansiering av terrorism när den förekommer i kombination med andra riskfaktorer, t.ex. om en betalning görs till ett högriskland (riskkategori geografi) och till kunder verksamma i en viss bransch, t.ex. i en kontantintensiv bransch (riskkategori kunder) (jfr 2 kap. 5 § andra punkten penningtvättslagen och Eba:s riktlinjer för riskfaktorer).

Illustration av hur en riskfaktor kan påverka risken med andra riskfaktorer

Bilden illustrerar att riskfaktorn gränsöverskridande transaktion kan påverka risken med andra riskfaktorer, t.ex. ett transaktionskonto där gränsöverskridande transaktioner är möjliga att genomföra.

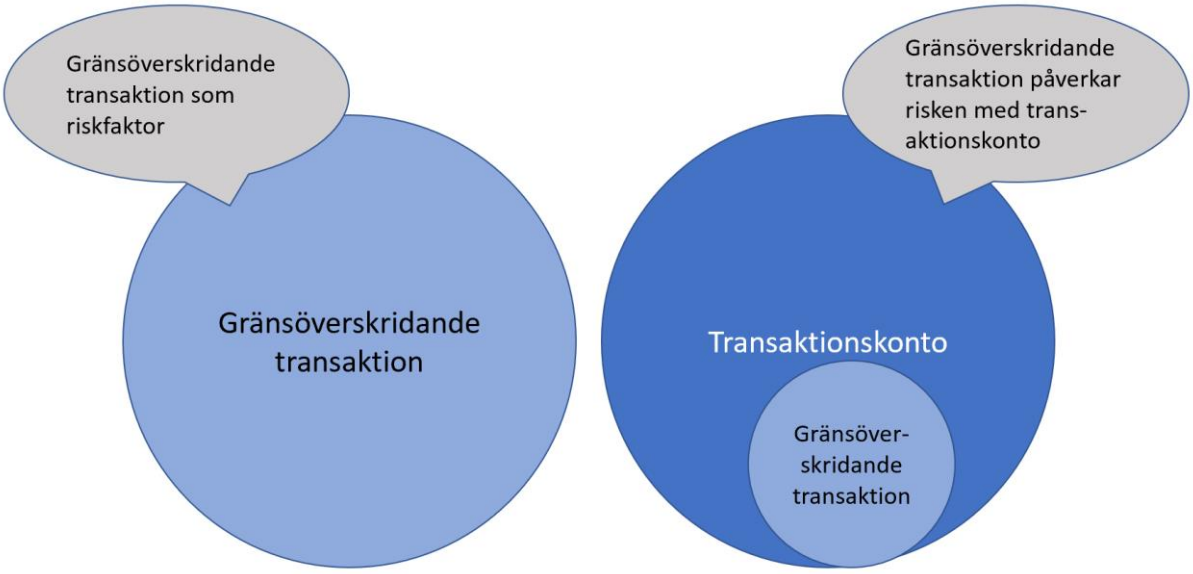


Illustration riskfaktorer kan påverka risken i kombination med varandra

Bilden illustrerar olika riskfaktorer – gränsöverskridande transaktion, transaktion till högriskland och till kunder i kontantintensiv bransch (högriskbransch) – som i kombination med varandra kan påverka risken för att verksamheten utnyttjas för penningtvätt och finansiering av terrorism.

Riskvärde och riskvikt

Riskfaktorerna kan åsättas ett värde, som indikerar i vilken omfattning faktorn innebär en risk för penningtvätt eller finansiering av terrorism. En riskfaktor kan innebära en viss risknivå sedd för sig själv, men i kombination med andra faktorer kan den innebära en annan nivå.

Riskvärdet grundar sig normalt sett på den information som verksamhetsutövaren har inhämtat via interna och externa källor. Framför allt de egna erfarenheterna kan innebära att olika verksamhetsutövare kan åsätta en och samma riskfaktor olika värde. Vissa riskfaktorer är dock särskilt reglerade. Exempelvis har riskfaktorn högrisktredjeland ett högt värde redan på den grunden att det följer av 3 kap. 17 § penningtvättslagen.

I Eba:s riktlinjer för riskfaktorer, riktlinjerna 3.4–3.7, beskrivs viktning av riskfaktorer. Där framgår bl.a. att när ett företag bedömer risken för penningtvätt och finansiering av terrorism kan det besluta att ge riskfaktorerna olika vikt utifrån deras relativa betydelse (riktlinje 3.4). När ett företag viktar riskfaktorer bör det göra en välgrundad bedömning av olika riskfaktorers betydelse i samband med en affärsförbindelse, en enstaka transaktion eller verksamheten. Denna resulterar ofta i att olika faktorer får olika ”poäng” (anm. ”scores” i den engelska språkversionen), vilket till exempel kan resultera i att en kunds personliga kopplingar till en jurisdiktion med högre risk för penningtvätt och finansiering av terrorism är mindre relevant med tanke på de egenskaper produkten i fråga har (riktlinje 3.5). I slutändan kommer sannolikt den vikt som tillmäts var och en av dessa faktorer att variera från produkt till produkt och från kund till kund (eller kundkategori) och från ett företag till ett annat. När ett företag viktar riskfaktorer bör det bl.a. säkerställa att viktningen inte påverkas på ett oönskat sätt av en enda faktor (riktlinje 3.6).

Steg 3: Bedöma sannolikhet, konsekvens och riskexponeringen

I Eba:s riktlinjer för riskfaktorer definieras risk som sannolikheten för att penningtvätt och finansiering av terrorism ska äga rum samt dess påverkan om så sker.

Det är inte reglerat hur sannolikhetsbedömningen ska göras. Sannolikhetsbedömningen handlar i praktiken om att göra en bedömning av hur stor sannolikheten är för att penningtvätt eller finansiering av terrorism ska äga rum genom ett utnyttjade av verksamheten. Bedömningen bör göras utifrån verksamhetens omfattning i relation till en riskfaktor. Bedömningen kan bygga på sådant som antalet kunder som använder en viss produkt eller tjänst. Det innebär med gränsöverskridande transaktioner som ett exempel att en bedömning kan göras av vilken i omfattning som gränsöverskridande transaktioner möjliggörs i verksamheten. Verksamhetsutövaren kan ha begränsat möjligheten att göra gränsöverskridande transaktioner i en sådan omfattning att det är endast sker ett fåtal per år, vilket kan innebära att sannolikheten för att utnyttjas är lägre än vad den annars hade varit. Ett annat exempel är riskfaktorn kunder i kontantintensiva branscher. Om verksamhetsutövaren endast har ett fåtal kunder i kontantintensiva branscher kan det minska sannolikheten för att penningtvätt eller finansiering ska äga rum.

Utöver sannolikhetsbedömningen görs en bedömning av den påverkan eller konsekvens som ett utnyttjade kan få. I den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2020/2021, s. 122, anges att begreppet *konsekvens* generellt sett syftar på den effekt eller skada som penningtvätt och finansiering av terrorism kan orsaka. Detta omfattar brottslighetens eller terrorismens påverkan på finansiella system och institut, liksom på ekonomin och samhället i stort. Konsekvenser är alltså den påverkan som penningtvätt och finansiering av terrorism kan orsaka på både kort och lång sikt, samt hur den kan påverka befolkningen, särskilda grupper, företagsklimat, nationella och internationella intressen samt finanssektorns rykte och attraktionskraft i ett land. Enligt Fatf behöver en riskbedömning inkludera en uppskattning av hot, sårbarheter och konsekvenser. Då det rent generellt är svårt att avgöra eller uppskatta konsekvenserna är det allmänt accepterat att en sådan analys inte måste gå på djupet, utan kan utgöra en helhetsbild av hotens och sårbarheternas konsekvenser för samhället.

I den nationella riskbedömningen handlar det om konsekvenser i ett större perspektiv. När en allmän riskbedömning görs av en verksamhet ligger det nära till hands att se till konsekvenserna i det större perspektivet, men också för verksamheten. Rent allmänt kan konstateras att det är allvarligt varje gång som verksamheten utnyttjas för penningtvätt eller finansiering av terrorism. Det kan dock vara svårt

att göra en detaljerad uppskattning och bedömning av konsekvenserna. Det blir i regel fråga om att göra en helhetsbedömning av hur allvarliga konsekvenserna kan bli vid ett utnyttjande, t.ex. om det kan bli fråga om stora belopp. Skulle exempelvis penningtvätt i vissa fall kunna ske av stora belopp, behöver sannolikheten inte bedömas vara särskilt hög för att risken ska bedömas som förhöjd. Vid bedömningen av konsekvenserna bör också de skillnader som finns i fråga om konsekvens vid penningtvätt jämfört med finansiering av terrorism beaktas.

Grundat på den bedömning av sannolikhet och konsekvens som har gjorts kan verksamhetsutövaren göra en sammantagen bedömning av sin riskexponering, vilket också kan beskrivas som den samlade riskbilden. Riskexponeringen kan bedömas på olika sätt. Det handlar i grunden om att titta på helheten; vilka risker som verksamheten faktiskt är exponerad för och hur stor risken i praktiken är, t.ex. utifrån hur många kunder som använder en högriskprodukt. Riskexponeringen är inte någon statisk bedömning utan varierar över tid beroende på vilka riskfaktorer som är aktuella.

Riskexponeringen kan inte bara bedömas på olika sätt utan kan också användas på olika sätt. Riskexponeringen kan utgöra grunden för att bedöma vilka åtgärder som måste vidtas för att hantera den risk som verksamheten är exponerad för. Om riskexponeringen är begränsad till ett fåtal kunder, kan vissa åtgärder vara både mer lämpliga och resurseffektiva än om riskexponeringen relaterar till tusentals kunder. Bedömningen ger en bild av de områden där verksamhetsutövaren behöver satsa mer resurser men även var företaget kan lägga mindre resurser.

Fas 2: Bedöma effektivitet i de mitigerande åtgärder som har vidtagits för att hantera den inneboende risken

Steg 1: Identifiera åtgärder

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 mitigera den inneboende risken. Detta ska göras i tillräcklig grad för att sedan kunna avgöra om en produkt eller tjänst ska kunna tillhandahållas en kund. Varje företag avgör vilka åtgärder som ska vidtas för att effektivt hantera riskerna.

Åtgärderna kan vara utformade på olika sätt. Det kan vara begränsningar av olika slag, t.ex. hur en produkt kan användas. Det kan också vara frågor som ställs till kunderna, åtgärder i övervakningen av transaktionerna eller utbildning av personalen.

Det bör framhållas att åtgärder kan beaktas på olika sätt. När den inneboende risken bedöms kan det – med produktriskbedömningen som exempel – beaktas t.ex. vilka inbyggda begränsningar som finns i riskfaktorerna. Det kan handla om sådant som hur en produkt är utformad, t.ex. beloppsbegränsningar, eller att ett konto endast kan användas för nationella transaktioner (dvs. inte möjliggör gränsöverskridande transaktioner). Motsvarande begränsningar kan finnas i förhållande till övriga riskkategorier, t.ex. distributionskanal. Olika begränsningar är dock också exempel på något som kan införas som åtgärder för att sänka den inneboende risken.

Steg 2: Bedöma utformning och effektivitet i åtgärderna

Efter att de mitigerande åtgärderna har vidtagits eller implementerats görs en bedömning av om de har varit effektiva. Det handlar om att kontrollera att åtgärderna har implementerats på avsett sätt och att åtgärdernas utformning (även kallat ”design”) har varit ändamålsenlig och därmed haft avsedd effekt. Det görs med andra ord en uppföljning och bedömning av om åtgärderna effektivt har mitigerat riskerna. Ytterst handlar det om att bedöma huruvida åtgärderna faktiskt har bidragit till en effektivare riskhantering, se också The Wolfsberg Group – Demonstrating Effectiveness [Publication of Wolfsberg Group statement on Demonstrating Effectiveness - Wolfsberg Group (wolfsberg-group.org)]

Uppföljningen bör vara riskbaserad, t.ex. i fråga om hur ofta den bör ske. Företaget bör ha rutiner för hur uppföljningen ska ske. Kontrollerna bör vara som starkast när det gäller de allvarligaste riskerna som har identifierats och kan vara enklare när det gäller mindre risker.

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

Om åtgärderna inte har haft avsedd effekt kan det t.ex. bero på att en åtgärd inte var rätt utformad eller hade rätt ”design” för ändamålet. Åtgärderna kan då behöva anpassas. Det kan också bero på brister i bedömningsunderlaget, t.ex. felaktiga antaganden om ett visst hot. Detta kan behöva omhändertas i utvärderingen av den allmänna riskbedömningen eller tidigare, om det behövs.

Exempel på mitigerande åtgärd och utvärdering av effektivitet

EXEMPEL PÅ MITIGERANDE ÅTGÄRD	EXEMPEL PÅ UTVÄRDERING AV EFFEKTIVITET
Kundkännedomsprocessen och bedömningen av kundens riskprofil (riskklass)	Hur fungerade inhämtningen av uppgifter? Hur fungerade bedömningen av inhämtade uppgifter? Här kan det också göras en bedömning av om det t.ex. har funnits tillräckliga resurser för att hantera processen och bedömningen. Hur fungerade riskklassificeringsprocessen? Visade uppföljningen att den riskprofil (riskklass) som kunden fick initialt stämde överens med kundens transaktioner och förväntade beteende?
Beloppsbegränsningar för t.ex. kontanter eller gränsöverskridande transaktioner	Har kundernas användning av produkten genererat färre avvikelser i transaktionsövervakningen än tidigare?
Transaktionsövervakningen/monitoreringen	Hur många ”larm” och rapporter till Finanspolisen gjordes under den bedömda perioden?

	Hur många ”larm” medförde en fördjupad granskning och hur många kunde stängas utan fördjupad granskning?
Utbildning och skydd av anställda	Vad visade utvärderingen av utbildningen? Vad blev resultatet av utbildningen, uppnåddes målen med utbildningen? Vad visade utvärderingen av skyddet av anställda?
Interna rutiner, riktlinjer och processer	Var rutinerna, riktlinjerna och processerna relevanta och effektiva? Hur fungerade och upprätthölls rutiner, riktlinjer och processer, skedde arbetet enligt dessa eller finns det brister i hur de följs? När det exempelvis finns en rutin som innebär att kunden måste ge in en särskild ansökan om att få genomföra och ta emot betalningar från ett visst land: • Hur många kunder fick ge in en ansökan? • Fanns det kunder som tilläts genomföra eller ta emot betalningar utan ansökan? Vad berodde i så fall det på? • Hade rutinen någon effekt på antalet ”larm” i monitoreringen? • Hur många kunder blev föremål för rapportering, trots ansökan?

Fas 3: Bedöma residualrisken

I Eba:s riktlinjer för riskfaktorer, riktlinje 1.3, framgår att när ett företag bedömer den kvarstående risknivån för penningtvätt och finansiering av terrorism som förknippas med verksamheten och enskilda affärsförbindelser eller enstaka transaktioner, bör det beakta såväl den inneboende risknivån som kvaliteten på kontroller och andra riskmitigerande faktorer.

Ett annat ord för den kvarstående risknivån är residualrisken. Residualrisken kan beskrivas som ett mått på hur stor risken för penningtvätt och finansiering av terrorism är efter att mitigerande åtgärder har vidtagits. Residualrisken är med andra ord ett mått på om risken har hanterats adekvat eller om det finns kvarstående risker, men är även ett mått på om det finns risker som är så pass stora att de inte kan hanteras, i varje fall inte utan ytterligare åtgärder.

Residualrisken kan falla inom eller utanför företagets riskaptit, dvs. den risknivå som företaget är berett att acceptera, se nedan.

Riskaptit

Riskaptit förekommer inte som begrepp i penningtvättslagen eller i penningtvättsföreskrifterna. Begreppet riskaptit förkommer dock i Eba:s riktlinjer för riskfaktorer, som gäller som allmänna råd. I riktlinjerna definieras begreppet som *den risknivå som ett företag är berett att acceptera* (avsnitt 2 punkten 12.j). Enligt riktlinje 4.7 g bör ett företag tydligt i sina riktlinjer och åtgärder ange sin riskaptit. I riktlinje 4.64 c anges som exempel på en skärpt åtgärd för kundkännedom att öka frekvensen av den fortlöpande övervakningen för att förvissa sig om att företaget fortsatt kan hantera risken med den enskilda affärsförbindelsen eller dra slutsatsen att förbindelsen inte längre motsvarar dess *riskaptit*, samt bidra till att identifiera transaktioner som behöver granskas närmare.

Riskaptit förekommer på andra ställen i regleringen på det finansiella området, bl.a. i Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut. I 2 kap. 3 § framgår att ett företag ska ha en dokumenterad riskaptit som omfattar företagets alla slag av risker. Styrelsen ska besluta om företagets riskaptit och regelbundet utvärdera riskaptiten och uppdatera den om det behövs.

Av beslutspromemorian till FFFS 2014:1[1] s. 18, framgår bl.a. följande. Riskaptiten bör adressera företagets väsentliga risker. Riskaptiten bör fungera som en spärr mot överdrivet risktagande och bör vara gränssättande för företagsledningen i dess arbete med att uppfylla företagets affärsstrategi. Riskaptiten bör vara framåtblickande och utsättas för scenarioanalyser och stresstester för att säkerställa att de som beslutar om riskaptiten samt övriga relevanta intressenter inom företaget (till exempel risktagare) förstår vilka händelser som skulle kunna medföra att företaget överskrider riskaptiten. Riskaptiten bör innehålla kvantitativa mått som kan överföras till risklimiter samt kvantitativa förlustmått/mått på negativa utfall, vilka ska kunna såväl aggregeras som delas upp.

Det kan uppfattas som motsägelsefullt att tala i termer av riskaptit och att acceptera risk på penningtvättsområdet, dvs. på ett område där regleringen syftar till att förhindra att verksamheten utnyttjas för penningtvätt och finansiering av terrorism. Det är dock inte realistiskt att utgå från att ett företag kan säkerställa att verksamheten aldrig utnyttjas för penningtvätt eller finansiering av terrorism. Det finns alltid risker med att driva verksamhet. Det riskbaserade regelverket innebär också att verksamhetsutövaren ska kunna ta risker, även höga risker, så länge som dessa kan hanteras.

För att kunna avgöra om residualrisken är inom riskaptiten och kan accepteras bör den vara mätbar och kunna jämföras med mätpunkter i riskaptiten. Det är viktigt att utgå från företagets egen kapacitet och förmåga att hantera risken. Ett exempel kan vara att mäta det antal transaktioner av ett visst slag som görs och jämföra det med det antal transaktioner (av samma slag) som företaget har kapacitet och förmåga att hantera och acceptera.

När residualrisken faller utanför riskaptiten kan det leda till att företaget fattar ett beslut om att inte tillhandahålla vissa produkter eller tjänster eller att inte vända sig till vissa marknader. Företaget kan, som ett alternativ, besluta att vidta åtgärder i syfte att hamna inom sin riskaptit, t.ex. begränsa möjligheten att genomföra vissa transaktioner eller skärpa övervakningen. Ett annat exempel är att införa olika rutiner, t.ex. en rutin som innebär att kunden måste ge in en särskild ansökan om att få genomföra och ta emot betalningar från ett visst land samt svara på vissa frågor. De åtgärder som vidtas i

[1] FI Dnr 11-5610 Nya regler om styrning, riskhantering och kontroll i kreditinstitut (fi.se)

syfte att hålla residualrisken på en nivå som ligger inom riskaptiten behöver utvärderas och kan behöva anpassas efter en förändrad riskbild.

Illustration av faserna 1-3 i metoden för att göra allmän riskbedömning

Hålla den allmänna riskbedömningen uppdaterad

Inledning

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 (2 kap. 1 § penningtvättsföreskrifterna). Det regleras inte när under året som utvärderingen ska göras. 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).

Företagets riskbedömning utgör grunden för företagets rutiner, riktlinjer och övriga åtgärder mot penningtvätt och finansiering av terrorism. Det är därför 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 verksamhetsutövaren 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).

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 andra fall går det bra att avvakta och hantera händelsen i samband med den årliga utvärderingen.

Den regelbundna utvärderingen och uppdateringen

Den regelbundna utvärderingen och uppdateringen innebär att det åtminstone årligen görs en total och samlad översyn av den allmänna riskbedömningen. 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 eller att riskerna har förändrats inom olika affärsområden. Det kan också visa sig att de mitigerande åtgärderna inte har haft avsedd effekt, vilket kan innebära att processen för att göra allmän riskbedömning behöver ses över.

Tillvägagångssätten vad gäller 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 ha en process för detta.

Uppdatering vid särskilda händelser

Utöver kravet på att minst årligen se över den allmänna riskbedömningen finns det flera särskilda händelser, både interna och externa, som innebär att den allmänna bedömningen behöver uppdateras (se 2 kap. 1 § penningtvättsföreskrifterna och illustrationen nedan). I dessa fall räcker det i regel med 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 regelbundna utvärderingen. Hela processen för att göra den allmänna riskbedömningen behöver alltså inte göras igen med anledning av att

en särskild händelse har inträffat. I vissa fall kan dock en större revidering behövas, särskilt vid större lagändringar som ställer nya krav.

Exempel på interna händelser

- **Lärdomar från verksamheten** – I verksamheten finns det mycket kunskap. Lärdomarna från verksamheten är viktiga att ta tillvara. Det handlar t.ex. om sådant som uppmärksammas i det löpande arbetet vid transaktionsövervakningen, rapporteringen till Finanspoliser och iakttagelser kring förändrade kundbeteenden.
- **Nya eller förändrade produkter eller tjänster** – När nya produkter och tjänster utvecklas ska risken för att produkten eller tjänsten utnyttjas för penningtvätt och finansiering av terrorism bedömas samt åtgärder vidtas för att mitigera riskerna.
- **Ny eller förändrad teknik eller process m.m.** – Processer som påverkar kundbeteenden, nya marknader/kunder, nya distributionskanaler, ny teknik, t.ex. digitalisering, omorganisation eller nya system kan bl.a. leda till att företagets sårbarhet ökar eller minskar. Det är viktigt att företaget analyserar vilka riskfaktorer som påverkas och vilka åtgärder som behöver vidtas.

Exempel på externa händelser

- **Omvärldsbevakning** – Omvärldsbevakningen handlar mycket om att uppmärksamma modus och trender och att hålla sig uppdaterad i fråga om rapporter och annat från myndigheter, t.ex. Finanspolisen och Säkerhetspolisen, den nationella riskbedömningen och beslut från Finansinspektionen.
- **Nya eller förändrade regelverk** – Nya eller förändrade regelverk kan indikera att riskfaktorer har förändrats. Det kan också innebära att vissa riskfaktorer förändras, t.ex. om ett regelverk bidrar till att en sårbarhet i systemet täpps till.

Illustration av det löpande arbetet med den allmänna riskbedömningen

Del II – Några processfrågor i arbetet med allmän riskbedömning

Inledning

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

Det är viktigt att verksamhetsutövaren 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.

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

Frågeställningarna utgår från olika delar av en process som omfattar ett förberedande arbete, att det sker en intern beredning, att den allmänna riskbedömningen fastställas och förankras samt att resultatet kommuniceras och implementeras.

Delar av processen för att göra den allmänna riskbedömningen

Vem har ansvar för den allmänna riskbedömningen?

Ansvaret för den allmänna riskbedömningen är regelverksstyrt. Om verksamhetsutövaren har en särskilt utsedd befattningshavare (SUB) enligt 6 kap. 2 § punkten 1 penningtvättslagen, 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 verksamhetsutövaren 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.

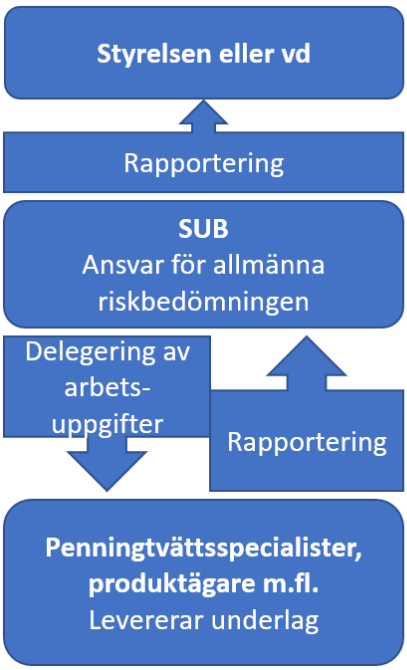
SUB ska rapportera till styrelsen eller vd. Om SUB är företagets vd, ska rapportering ske till styrelsen (6 kap. 4 § penningtvättsföreskrifterna). Att rapportering sker uppåt i organisationen är viktigt även i de fall delegering av arbetsuppgifter har skett. Det arbete som i förekommande fall penningtvätts-specialisterna, 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 bl.a. 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.

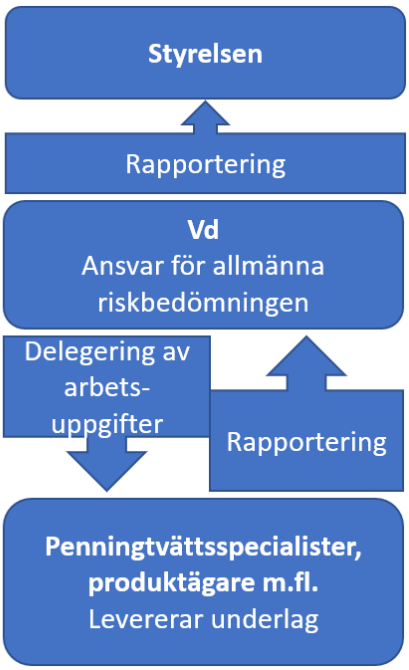
Illustration ansvar, rapportering och delegering

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 och som har ansvaret.

När det finns SUB



När det inte finns SUB



Vilka förberedande åtgärder vidtas?

Verksamhetsutövaren bör ha en tydlig metod och process för arbetet med att göra allmän riskbedömning. Metoden och processen bör vara utformad på ett sätt som gör det enkelt att följa upp att alla moment är genomförda, att processen har fungerat och 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 som hindrar att befintliga processer används 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.

I arbetet med den allmänna riskbedömningen kan det vara lämpligt med workshops där flera funktioner i företaget deltar. Generellt sett är det viktigt att sammanställa och dokumentera den data och analys, dvs. det underliggande arbete som har resulterat i riskbedömningen för att i efterhand kunna se vad som har påverkat den. Dokumentationen kan även användas som en form av kontrollbevis för att arbetet har utförts.

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.

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.

Hur bereds och presenteras allmänna riskbedömningen?

Det kan vara lämpligt med en rutin för att säkerställa att alla moment i processen för att göra den allmänna riskbedömningen är genomförda. När flera funktioner i företaget har varit involverade i arbetet med den allmänna riskbedömningen kan det också vara lämpligt med en intern beredning, 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 berörda personer i företaget.

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.

Den allmänna riskbedömningen 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 vilka mitigerande åtgärder som ska vidtas, allokera resurser, bestämma kundens riskprofil och inriktningen och omfattningen av övervakningen. Den kan också användas när en ny produkt eller tjänst tas fram (i 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.

Företaget kan dela upp den allmänna riskbedömningen i olika delar eller dokument. Detta kan t.ex. göras för att företaget vill hantera vissa delar på ett mindre exponerat sätt än andra delar.

Hur fastställs och förankras allmänna riskbedömningen?

Den allmänna riskbedömningen ska dokumenteras (2 kap. 2 § penningtvättslagen). Detta kan göras på olika sätt. 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 också ett viktigt stöd för verksamhetsutövare att vidta vissa åtgärder och för att åtgärder inte vidtas i vissa situationer.

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 och behov av mitigerande åtgärder är en nödvändig förutsättning för att ledningspersoner ska kunna fatta välinformerade beslut.

Hur kommuniceras och implementeras allmänna riskbedömningen?

Det finns vissa regelverksstyrda krav varigenom den allmänna riskbedömningen i praktiken kommuniceras i företaget:

- Enligt 2 kap. 8 § penningtvättslagen ska verksamhetsutövaren 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.
- Kravet på utbildning och information i 2 kap. 14 § penningtvättslagen omfattar den allmänna riskbedömningen.

Det är viktigt att resultatet av den allmänna riskbedömningen kommuniceras till alla delar i företaget som påverkas av det, jfr den krets som omfattas av utbildningskravet i 2 kap. 14 § penningtvättslagen. Det innebär att den kommuniceras till kundansvariga, produktägare och vd, dvs. i princip samma funktioner som på olika sätt har varit delaktiga i framtagandet av riskbedömningen samt till andra som på olika sätt berörs av den.

Verksamhetsutövaren 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. 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 bl.a. 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.